# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/724,734 | 11/28/2000 | Stephen M. Trimberger | X-805-8 US | 7773 |

24309 7590 11/15/2005

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

| EXAMINER | |
|---|---|
| LEMMA, SAMSON B | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/724,734 | TRIMBERGER ET AL | |
| | Examiner | Art Unit | |
| | Samson B. Lemma | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *10 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are ~~withdrawn from consideration~~.

5)☒ Claim(s) *9-13* is/are allowed.

6)☒ Claim(s) *1-8 and 14-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *03/05, 01/05, 10/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## *DETAILED ACTION*

1. This office action is in replay to an amendment filed on August 10, 2005. Independent claim 9 has been amended. Dependent claims 10-17 have been amended too and **claims 1-20** are pending.

### *Information Disclosure Statement*

2. Applicants request for the consideration of the Information Disclosure Statement filed is acknowledged. Examiner has reviewed and signed all copies of the IDS submitted.

## *Response to Arguments*

3. Applicant's remark/arguments filed on August 10, 2005 regarding claims 1-8 and 14-20 have been fully considered but they are not persuasive.

**Applicant first argument is based on the limitation in the independent claim 1.**

Applicants made the following remark in support of the amendment, "Claim 1 includes limitations of a configuration bitstream including a plurality of unencrypted words for controlling loading of configuration data in combination with a plurality of encrypted words that specify the encrypted design. This combination of limitations is not shown to be suggested by the Trimberger-Erickson combination.

Neither of Trimberger nor Erickson is shown suggest that part of a configuration bitstream is encrypted in combination with part of the configuration bitstream being unencrypted. Trimberger teaches control words and configuration, data, both being unencrypted, and Erickson is cited as teaching encrypted configuration data. Trimberger and Erickson do not, however, suggest the claimed combination of part of the configuration bitstream being unencrypted and part of the configuration bitstream being encrypted. Trimberger teaches all of the configuration bitstream is unencrypted, both programming instructions and configuration data. Erickson does not appear to distinguish between different parts of a configuration bitstream and generally teaches configuration stream encryption (Title, Abstract). Thus, Trimberger does not encrypt anything, and Erickson appears to encrypt all of a configuration bitstream.

**Examiner disagrees with this argument**.

Examiner would first of all points out that the secondary reference namely Erickson discloses the following, "In another embodiment, **at least a portion of the configuration data 130 is encrypted by the software tools before being stored in the storage device 120 and the encryption circuit 125 further encrypts the already encrypted data."[Column 4, lines 24-27].** This inherently implies **that portion of configuration data is encrypted and part of the configuration left unencrypted.**

Erickson further discloses that the encryption circuit 125 further encrypts only the already encrypted data. The security circuit 111 performs a

complementary double decryption to generate the configuration data needed to program the configurable logic elements 118.[Column 4, lines 27-31]

**Applicant second argument is based on the motivation used to combine** the two references on claim 1. Applicant argued that, the motivation for modifying **Trimberger with Erickson** for making claim 1 is improper because it lacks supporting evidence and is based on hindsight.

**Examiner disagrees with this argument,** Examiner would point out that It is not necessary that the reference actually suggest, expressly or in so many words, the changes or improvements that applicant has made. The text for combining references is what the references as a whole would have suggested to one of ordinary skill in the art. See In re Sheckle, 168 USPQ 716 (CCPA 1971) In re McLaghin 170 USPQ 209 (CCPA 1971). In re Young 159 USPQ 725 (CCPA 1968).

**Applicant third argument is with respect to the dependent claim 2. Applicant** argued that claim 2 includes limitations of one of the unencrypted words comprising a key address for locating a decryption key for decrypting the encrypted words. The cited portion of Erickson alleged to suggest these limitations contains no apparent relevance to a key address being part of the unencrypted words of a configuration bitstream. The cited teaching of Erickson simply teaches using a decryption key to decrypt configuration data. There is no apparent teaching by Erickson that the decryption key is addressed by part of the configuration bitstream. If the rejection is maintained, further explanation is requested.

**Examiner disagrees with this argument,** Examiner would point out that **Erickson** discloses that the decryption circuits 115 uses the key 180 from the security initialization circuit 114 to decrypt the encrypted configuration data 135, this implies that it would be obvious for one of ordinary skill in the art to add a key address in the unencrypted words so that the key in the initialization circuit 114 is activated to decrypt the encrypted configuration data. This feature is not patentably distinguishable.

**Applicant fourth argument is with respect to the dependent claim 6-8.**

Applicant wrote the following in support of his argument.

"The rejection of claims 6-8 over the Trimberger-Erickson-Kwiat combination should be withdrawn because the Office Action fails to show a suggestion of all the limitations and fails to provide a proper motivation for combining the references."

**Examiner disagrees with this argument,** Examiner would point out that all the limitation is disclosed in the combination of the three reference used as indicated below on the office action and it is not necessary that the references actually suggest, expressly or in so many words, the changes or improvements that applicant has made. The text for combining references is what the references as a whole would have suggested to one of ordinary skill in the art. See In re Sheckle, 168 USPQ 716 (CCPA 1971) In re McLaghin 170 USPQ 209 (CCPA 1971). In re Young 159 USPQ 725 (CCPA 1968).

**Applicant fifth argument is with respect to the dependent claim 15.**

**Examiner disagrees with this argument,** Examiner response provided to the dependent claims 6 and 8 above is also applicable to this argument as the core

of the argument is concerned with the motivation for combining the references used in the rejection.

**Applicant next argument is with respect to the dependent claims 18-20.**

Applicant wrote the following in support of his argument.

"The Office Action does not establish that claims 18-20 are unpatentable under 35 USC 103(a) over Erickson in view of Yin. The rejection is respectfully traversed because the Office Action fails to show that all the limitations are suggested by the references and fails to provide a proper motivation for modifying the teachings of Erickson with teachings of Yin. No suggestion is shown of forming a cipher block chaining initial value comprising a starting address for loading a design into a PLD. None of the cited teachings in either of the references appear to reference **this specific use of the starting address**. The Office Action also fails to provide a proper motivation for combining Yin with Erickson.

**Examiner disagrees with this argument,** Examiner asserts **Yin** discloses the steps of cipher block chaining of encryption comprising the steps of: Forming a cipher block chaining initial value comprising a starting address for loading a design into a PLD; (Column 5, lines 33-45; column 8, lines 59-67; figure 2b, ref. Num 42) (the 64 bit initial vector IV which is shown on figure 2b, ref. Num "42", is starting address for loading a design or predetermined sequences of bits into a PHE OR PLD as explained on column 7, lines 60-65 and column 8, lines 59-67). As to the argument raised by the applicant towards the motivation, the response provided to the dependent claims 6 and 8 above is also applicable to this argument as the core argument is concerned with the motivation for combining the references used in the rejection.

**Applicant's last argument is regarding the rest of the dependent claims.**

Applicants argued that since the independent claims are patentable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claims.

**In response to the above argument by the applicant, the examiner** reponse discussed for the independent claims above is also valid towards this argument.

Therefore all the elements of the limitations is explicitly or implicitly suggested and disclosed by the combinations of the references on the records and the rejection made to claims 1-8 and14-20 remains valid.

## *Claim Rejections - 35 USC § 103*

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-5 and 14,16,17** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen M. Trimberger** (hereinafter referred as **Trimberger)** (U.S. Patent No 5,892,961) **in view of Erickson et al** (hereinafter referred to as **Erickson**) (U.S. **Patent No. 5, 970,142) (Patent Date: October 19, 1999)**

6. **As per claim 1, Trimberger** discloses

- A bit stream for configuring a PLD with an encoded design comprising: (Column 2, lines 40-49; column 4, lines 10-21) (The design of the PLD which is

in the form of encoded bitstream includes the programming instruction and the configuration data for configuring the PLD or the "FPGA" as explained on column 2, lines 40-49; column 4, lines 10-21)

- A plurality of unencrypted words for controlling loading of configuration data; (Figure 3, column 5, lines 1-31; column 5, lines 44-60) (The submitted disclosure on page 11, lines 13-15, and on figure 2d and figure 4d by the applicant teaches the control words or data with a particular configuration logic register addresses are used for controlling the loading of the configuration data. Example given by the applicant such as bitstream header configuration address "0001" which represents the frame address is used for controlling the loading of configuration data. In fact all the configuration addresses shown on figure 2d and figure 4d with the exception of the configuration address "0010" and "0011" are considered and explained to be control data by the applicant since they are used for controlling loading of configuration data as explained on the submitted disclosure on page 11, lines 13-15. **Trimberger** on figure 3 and column 5, lines 1-31; column 5, lines 44-60 discloses a plurality of unencrypted bitstream or words which includes encoded instruction and then decoded by the CPU. These plurality of unencrypted words contains the op codes which represents a particular instruction used for controlling the loading of configuration data. For instance the word or bitstream which contains the "LF" op code which represents the instruction "Load Frame Immediate" is decoded by the CPU and this unencrypted word is used for controlling the configuration data by loading the data word onto the frame data path as explained on column 5, lines 1-14. On the top of that the unencrypted word or decoded word that contains the op codes "LFN N", represents "Load N bits", into frame register is also used for

controlling the configuration data by loading these N bits onto the frame data path as explained on column 5, lines 15-20) and

**Trimberger** does not explicitly disclose

- A plurality of encrypted words specifying the encrypted design.

However, in the same field of endeavor, **Erickson** discloses

A plurality of encrypted words or information or configuration data or design is transmitted from the storage device to the PLD and these encrypted words are used for specifying the encrypted design or the encrypted configuration data such that when the encrypted design or the encrypted configuration data is decrypted at the PLD, the resulting information is used for configuring the PLD.(Column 1, lines 59-column 2, line 5)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine a plurality of encrypted words specifying the encrypted design as per teaching of Erickson in to the method taught **Trimberger** in order for securing data used to configure a PLD. [See Erickson, column 1, lines 5-9]

7. **As per claim 2, Trimberger** on figure 3 and column 5, lines 1-31; column 5, lines 44-60 discloses the a plurality of unencrypted or decoded bitstream or words which includes instructions which are decoded or unencrypted by the CPU and these plurality of unencrypted words contains the op code which represents a particular instruction used for controlling the loading of configuration data. Example the word or bitstream which contains the "LF" op code which represents the instruction "Load Frame Immediate" is decoded by the CPU and this decoded or unencrypted word is used for controlling the configuration data by loading the data word onto the frame data

path as explained on column 5, lines 1-14)( figure 3, Column 5, lines 1-31; column 5, lines 44-60)

**Trimberger** further discloses that the exemplary instruction which is found by decoding the encoded bitstream or words and the result of which is decoded or unencrypted bitstream contains op codes which represents a particular instruction are listed on figure 3, but does not represent the totality of possible instructions which the CPU 40 can decode and implements. (Column 5, lines 54-61)

**Trimberger** does not explicitly disclose

- The bitstream of Claim 1 wherein one of the unencrypted words comprises a key address for locating a decryption key for decrypting the encrypted words

However, in the same field of endeavor, **Erickson** discloses

The decryption circuit uses or locate the decryption key from the security initialization circuit to decrypt the encrypted configuration data or word . (Column 3, lines 36-39)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ the locating of the decryption key for decrypting the encrypted word as per teachings of Erickson in to the method of as taught by Trimberger for the purpose of decrypting the encrypted control words.

8. **As per claim 3,** the combination of **Trimberger and Erickson** discloses the bitstream as applied to claim 1 above. **Furthermore, Trimberger** discloses the bitstream wherein one of the unencrypted words comprises an address register for loading the first word of the encoded design.(Column 2, lines 20-23)

9. **As per claim 4 and 5**, the combination of **Trimberger and Erickson** discloses the bitstream as applied to claims 1 and 4 above. Furthermore, **Trimberger discloses** the bitstream comprising a plurality of encrypted words for controlling loading of configuration data, wherein one of the encrypted words for controlling loading of configuration data specifies an address for loading a word of the encrypted design.(Figure 3, Column 5, lines 32-43) (The submitted disclosure on page 11, lines 10-13, and on figure 2d and figure 4d by the applicant teaches the word or data with a particular configuration logic register addresses namely addresses "0010" or Frame Data Input or "0011" or Frame Data Output are used for specifying the encrypted design. **Trimberger** discloses a plurality of encoded words shown on figure 3 which caries instructions such as "RD X" which instruct the CPU to read and the encoded word or data which contains the "RB" op code which represents read back instruction are both received by the CPU and used for specifying the encoded design as explained on column 5, lines 32-43 and shown on figure 3. On the top of that Erickson describes that these encoded words or data which contains the configuration data are actually encrypted as explained on column 1, lines 65-67; column 2, lines 1-13)

10. **As per claim 14**, the combination of **Trimberger and Ericksion** discloses the bitstream as applied to claim 1 above. Furthermore, **Trimberger** discloses the bitstream, wherein each plurality of encrypted words further specifies an address into which the encrypted design is to be loaded.(Column 3, lines 34-41)(the configuration logic elements could specifies the address for the purpose of configuring the PLD and meets the recitation of this claim).

11. **As per claim 16 and 17**, the combination of **Trimberger and Ericksion** discloses the bitstream as applied to claim 1 above. Furthermore, **Trimberger** discloses the bitstream, wherein each plurality of encoded words specifies the encoded design are

loaded into a single group or a plurality of groups of successive addresses. (Column 2, lines 49-54; Column 5, lines 15-21; Column 5, lines 21-31)(Erickson on the top of that discloses that the encoded words can actually be encrypted as explained on column 1, line 59-column 2, lines 5 and the combination of the two meets the recitation of the claim)

12. **Claims 6-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen M. Trimberger** (hereinafter referred as **Trimberger**) (U.S. Patent No 5,892,961) **in view of Erickson et al** (hereinafter referred to as **Erickson**) (U.S. **Patent No. 5, 970,142) (Patent Date: October 19, 1999)** further in view of **Kwiat** (hereinafter referred to as **Kwiat**) (U.S. Patent No. 5,931,959)

13. **As per claim 6**, The combination of **Trimberger and Erickson** discloses a method as applied to claim 1 above. Furthermore **Trimberger** discloses plurality of unencrypted bitstream or words which includes encoded instruction and decoded by the CPU and these plurality of unencrypted words contain the opcode which represents a particular instruction used for controlling the loading of configuration data. Example. The word or bitstream which contains the "LF" opcode which represents the instruction "Load Frame Immediate" is decoded by the CPU and this unencrypted word is used for controlling the configuration data by loading the data word onto the frame data path as explained on column 5, lines 1-14)( Figure 3, Column 5, lines 1-31; column 5, lines 44-60)

**The combination of Trimberger and Erickson does not** explicitly disclose

- The bitstream wherein the unencrypted words for controlling loading of configuration data include a cyclic redundancy checksum for comparison to a cyclic redundancy checksum calculated by the PLD.

However, in the same field of endeavor, **Kwiat** discloses a cyclic redundancy checksum for comparison to a cyclic redundancy checksum calculated by the PLD.( Column 10, lines 50-55)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine a Cyclic redundancy checksum (CRC) as per teaching of **Kwiat** in to the method of as taught by the combination of Trimberger and Erickson, in order to increase the chance of providing error free configuration of the PLD or FPGA when the design in the form of bitstream is loaded on to the PLD or FPGA.

14. **As per claims 7 and 8**, the combination of **Trimberger , Erickson and Kwiat** discloses the bitstream as applied to claim 6 above. Furthermore, **Kwiat** discloses the bitstream, wherein the cyclic redundancy checksum in the bitstream is calculated on configuration data after or before the configuration data has been encrypted. .( Column 16, lines 50-55)

15. **Claim 15** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen M. Trimberger** (hereinafter referred as **Trimberger**) (U.S. Patent No 5,892,961) in view of **Erickson et al** (hereinafter referred to as **Erickson**) (U.S. **Patent No. 5, 970,142) (Patent Date: October 19, 1999)** further in view of **John Yin** (hereinafter referred as **Yin**) (U.S. Patent No 6,028,939)

16. **As per claim 15**, the combination of **Trimberger and Erickson**, discloses the method as applied to claim 1 above. Furthermore **Trimberger** discloses each plurality of unencrypted bitstream or words which includes encoded instruction and decoded by the CPU and these plurality of unencrypted words contain the opcode which represents a particular instruction used for controlling the loading of configuration data. Example. The word or bitstream which contains the "LF" opcode which represents the instruction

"Load Frame Immediate" is decoded by the CPU and this unencrypted word is used for controlling the configuration data by loading the data word onto the frame data path as explained on column 5, lines 1-14)( figure 3, Column 5, lines 1-31; column 5, lines 44-60)

The combination of **Trimberger** and **Erickson** does not explicitly disclose
The bitstream wherein the plurality of unencrypted words for controlling loading of configuration data include a cipher block chaining initial value.
However, in the same field of endeavor, **Yin** discloses
The 64 bit initial vector IV which is shown on figure 2b, ref. Num 42, is starting address for loading a design or predetermined sequences of bits into a PHE OR PLD as explained on column 7, lines 60-65 and column 8, lines 59-67)( Column 5, lines 33-45; column8, lines 59-67; figure 2b, ref. Num 42)
Furthermore Yin discloses
The first word of design "Do" which is shown on figure 2b is combined or Xored with the cipher block initial value which is interpreted by the office to be IV at figure 2, ref. Num "40"(figure 2)
It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ the inclusion of cipher block chaining initial value as per teachings of **Yin** in to the method of as taught by the combination of **Trimberger and Erickson** for the purpose of strengthening the security of the PLD since a single bit error in a ciphertext block affects the decryption of all subsequent blocks.

17. **Claims 18-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Erickson et al** (U.S. **Patent No. 5, 970,142) (Patent Date: October 19, 1999)** further in view of **John Yin** (hereinafter referred **as Yin**) (U.S. Patent No 6,028,939)

18. **As per claim 18, Erickson** discloses

- A method of generating a bit stream with encrypted design data.(Column 1, line 59-column 2, line 5)

**Erickson** does not explicitly disclose forming a cipher block chaining encryption.

However, in the same field of endeavor, **Yin** discloses the steps of cipher block chaining of encryption comprising the steps of:

- Forming a cipher block chaining initial value comprising a starting address for loading a design into a PLD; (Column 5, lines 33-45; column 8, lines 59-67; figure 2b, ref. Num 42) (the 64 bit initial vector IV which is shown on figure 2b, ref. Num "42", is starting address for loading a design or predetermined sequences of bits into a PHE OR PLD as explained on column 7, lines 60-65 and column 8, lines 59-67)

- Combining the cipher block chaining initial value with a first word of design data to form a first combined word; (column 5, lines 33-45; column 8, lines 59-67; figure 2b, ref. Num "40") (The first word of design "Do" which is shown on figure 2b is combined or XORed with the cipher block initial value which is interpreted by the office to be "IV" to form a first word of design data which is interpreted by the office to be "Co" which is shown at figure 2b, ref Num "Co" meets the recitation of this claim)
- Encrypting the first combined word to form a first word of encrypted data; (Column 5, lines 33-45; column 8, lines 59-67; figure 2b) (The first combined word which is equivalent to "Co" is XORed on figure

2b, ref. Num 40 with the next encrypted bitstream data "D1" to form a first word of encrypted data which is interpreted by the office to be "C1")

- Combining the first word of encrypted data with a second word of design data to form a second combined word; (Column 5, lines 33-45; column 8, lines 59-67; figure 2b) (As shown on figure 2b, the second word of design data is "Di" is encrypted and XORed with "C1" which is interpreted by the office as the first word of encrypted data to form a second combined word which is interpreted by the office to be "Ci" and this meets the recitation of the claim) and

- Encrypting the second combined word to form a second word of encrypted data. (Column 5, lines 33-45; column 8, lines 59-67; figure 2b) (The second combined word which is interpreted by the office to be "Ci" shown at figure 2b will continue to be XORed with next design encrypted data "Di" and form a second word of encrypted data and this meets the recitation of this claim)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to encrypt the control word in chain block mode as per teachings of **Yin** in to the encryption method as taught by **Erickson** in order to enable a cost-effective, scaleable and high performance implementation of data security.[See Yin, column 5, lines 6-8]

19. **As per claim 19,** the combination of **Erickson and Yin** discloses the bitstream as applied to claim 1 above. Furthermore, **Yin d**iscloses the bitstream wherein, subsequent steps of combining and encrypting are repeated until all design data has been encrypted. (figure 2b; Column 5, lines 33-45; column 8, lines 59-67)

20. **As per claim 20**, the combination of **Yin and Erickson** discloses the bitstream as applied to claim 1 above. Furthermore, **Yin discloses** the bitstream wherein, the cipher block chaining initial value comprises further bits not part of the starting address for loading a design into a PLD. (Figure 2b; Column 5, lines 33-45; column 8, lines 59-67)

## *Allowable Subject Matter*

21. **Claims 9-13** are allowed.

## *Conclusion*

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a)

will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

11/02/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100